IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

LISA WHITE, individually and on behalf all others similarly situated, Plaintiff, v. THE UNITED NETWORK FOR ORGAN SHARING, Defendant.	**CASE NO. 3:24cv629** **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Lisa White ("Plaintiff") brings this action on behalf of herself and all others similarly situated against The United Network for Organ Sharing ("UNOS") ("Defendant"). Plaintiff seeks to obtain damages, restitution, and injunctive relief for a class of individuals ("Class" or "Class Members") who are similarly situated and have received notices of the data breach from UNOS. Plaintiff makes the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

I. NATURE OF THE ACTION

1. This class action arises out of a 2023 data breach ("Data Breach") of documents and information stored on the computer network of UNOS, a company that operates the organ transplant and donation process across the United States.

2. On its computer network, UNOS holds and stores certain highly sensitive personally identifiable information ("PII") and HIPAA protected health information ("PHI") (together "Private Information") of the Plaintiff and the putative Class Members, who are citizens either registered as an organ donors or those formerly or presently in need of organ donations as recipients, i.e., individuals who provided their highly sensitive and private information in exchange for organ donation and recipient services.

3. According to the Notice of Data Breach Letter that UNOS sent to Plaintiff and Class members, UNOS first became aware of the Data Breach on November 10, 2023, and began investigating.[1]

4. UNOS finally began notifying the unknown or undisclosed number of victims on or about August 21, 2024, nearly 10 months after the data breach occurred, stating that their PII had been exposed in what Defendant calls a "data privacy incident."[2]

5. UNOS also admits that it "is currently investigating a configuration error that may have permitted access by authorized users to some patients' personal and health information stored within two UNOS IT environments." and that it also revealed that "[u]pon discovery of the configuration error, we immediately initiated

---

[1] *See* Plaintiff's Notice Letter, attached as Exhibit A.
[2] *Id.*

a comprehensive response in accordance with our established IT procedures."[3]

6. According to a letter sent by Senators Ron Wyden and Chuck Grassley, "[o]n November 10, 2023, during two software tests, the United Network for Organ Sharing (UNOS) discovered it had been exposed to a data breach as a result of a software configuration error that gave unauthorized access to **at least 1.5 million patient records** to Organ Procurement and Transplantation Network (OPTN) and DonorNet system users."[4]

7. As a result of UNOS's Data Breach, Plaintiff and over a million Class Members suffered ascertainable losses in the form of financial losses resulting from identity theft, out-of-pocket expenses, the loss of the benefit of their bargain, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

8. In addition, Plaintiff's and Class Members' highly sensitive personal information—which was entrusted to Defendant—who claims that it "is committed to keeping information confidential and secure"[5]—was compromised and unlawfully accessed and extracted during the Data Breach.

9. Based upon UNOS's website notification and its notice letter, the Private Information compromised in the Data Breach was exposed due to its lack of

---

[3] https://unos.org/media-resources/releases/unos-statement-on-testing-environment-situation/ (last accessed September 3, 2024).
[4] https://www.grassley.senate.gov/news/news-releases/grassley-wyden-probe-data-breach-that-exposed-organ-transplant-patients-sensitive-data (last accessed September 5, 2024).
[5] https://unos.org/privacy-policy/ (last accessed September 5, 2024).

proper security and appropriate system configuration, which allowed unauthorized access to Plaintiff's and the Class Members' highly sensitive PII and PHI stored on UNOS's network.

10. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiff and Class Members' Private Information.

11. Upon information and belief, Defendant was aware of its inadequate computer network systems at least since January of 2022. The Senate Finance Committee stressed its concerns about Defendant's lax computer security and the risk of lethal harm to medically fragile patients in a letter to UNOS dated March 20, 2023:

> On January 31, 2022, we wrote to your organization expressing concerns and asking then CEO Brian Shepard to, "[t]ake immediate action to modernize the national Organ Procurement and Transplantation Network (OPTN) information technology system and secure it from cyber-attacks." On February 11, 2022, we also wrote to the White House Chief Information Officer voicing our concerns about the cybersecurity and technology used by UNOS as the nation's Organ Procurement and Transplantation Network (OPTN) contractor.[6]

12. Plaintiff brings this class action lawsuit on behalf of herself and those similarly situated to address Defendant's inadequate safeguarding of Class

[6] https://www.grassley.senate.gov/news/news-releases/grassley-praises-hhs-action-to-restore-integrity-in-life-saving-organ-transplant-system (*See* link to letter) (last accessed September 3, 2024).

Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the exposure of an unknown third party and precisely what specific type of information was accessed.

13. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks and openly accessible to unauthorized persons. The mechanism and risks associated with the unauthorized exposure of Plaintiff's and Class Members' Private Information was a known risk to Defendant. Thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left Plaintiff's and Class Members' property in a dangerous condition.

14. Defendant disregarded the privacy and property rights of Plaintiff and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions and exposure; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; failing to promptly address repeated concerns that were expressed in letters from the U.S. Senate committee; and failing

to provide Plaintiff and Class Members prompt and accurate and complete notice of the Data Breach.

15. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its computers, it would have discovered the insecurities of its system and detected the exposure sooner, and potentially been able to mitigate the injuries to Plaintiff and the Class.

16. Plaintiff's and Class Members' identities are now at substantial and imminent risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained (including Social Security numbers) is now in the hands of data thieves.

17. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

18. As a result of the Data Breach, Plaintiff and Class Members have been

exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their medical and financial accounts to guard against identity theft.

19. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft, as well as losing valuable time that can be used for other productive purposes.

20. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach (the "Class").

21. Accordingly, Plaintiff brings this action against Defendant for negligence, breach of implied contract, unjust enrichment, and declaratory relief, seeking redress for UNOS's unlawful conduct.

22. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs and for lost time, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate, long term credit monitoring services funded by Defendant, and declaratory relief.

II. PARTIES

23. Plaintiff Lisa White is and at all times relevant to this Complaint an

individual citizen and resident of the State of Tennessee. Plaintiff White received a Notice of the Data Breach from UNOS dated August 21, 2024, and attached as Exhibit A (the "Notice Letter").

24. UNOS is a private corporation organized and headquartered in Richmond, Virginia. UNOS's principal place of business is located at 700 N 4th Street, Richmond, Virginia 23219.

III. JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiff White, is a citizen of a state different from Defendant.

26. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business or business venture in this State; it is registered with the Secretary of State as a domestic non-stock corporation; it maintains its headquarters in Virginia; and committed tortious acts in Virginia.

27. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the district within which UNOS has the most significant contacts.

IV. STATEMENT OF FACTS

Nature of Defendant's Business.

28. UNOS claims it "was founded to help the community of donation and transplant professionals make the best possible use of organs to save lives." It has been providing organ transplant services since 1984.[7]

29. UNOS states "UNOS has grown from a handful of staff in rented office space to an organization with more than 450 employees."[8]

30. UNOS states it "encompasses not only donation and transplant but also broader public health projects through its work developing new technologies and initiatives, conducting data-driven research and analysis, providing expert consulting services, advocating for patients, and being a leader in bringing communities together to save lives."[9]

31. People provided UNOS with their PII with the mutual understanding that this highly sensitive private information was confidential and would be properly safeguarded from misuse and theft.

32. UNOS (falsely) promises in its Privacy Policy that "the data we collect are securely stored on our servers according to industry standards and best practices

[7] https://unos.org/about/history-of-unos/ (last accessed September 3, 2024).
[8] *Id.* (last accessed September 3, 2024).
[9] *Id.*

for security."[10]

33. In the course of collecting Private Information from consumers, including Plaintiff and Class Members, UNOS promised to provide confidentiality and adequate security for Private Information through its applicable Privacy Policy and in compliance with statutory privacy requirements applicable to its industry. UNOS is aware of and had obligations created by HIPAA, FTCA, statute, contract, industry standards, and common law to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access, exposure, and disclosure.

34. Plaintiff and the Class Members, as individuals and consumers, relied on the promises and duties of UNOS to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

35. Consumers, in general, demand that businesses that require highly sensitive PII and PHI will provide security to safeguard their Private Information, especially when Social Security numbers and especially sensitive health information are involved.

36. In the course of their dealings, including Plaintiff and Class Members,

[10] https://unos.org/privacy-policy/

provided UNOS with all or most of the following types of Private Information:

- First and last names;
- Home addresses;
- Dates of birth;
- Financial information;
- Photo identification and/or driver's licenses;
- Email addresses;
- Phone numbers;
- Social Security numbers.
- Relationship Status;
- Bank account and/or payment card information; and
- Extensive protected health information.

37. UNOS had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII and PHI from unauthorized disclosure to third parties.

The Data Breach.

38. According to its Notice Letters to those affected, on November 10, 2023, UNOS became aware of unauthorized exposure to Private Information on its servers. After an unspecified amount of time, between the date they became aware and when they sent the notice letters, its investigation determined that "users of the test environments had access to private information instead of test data" since their

creation in 2007 and 2011.[11]

39. The letter specifies that that the exposure was discovered on UNOS's network sometime around November 10, 2023, when the investigation showed that unauthorized individuals were able to view the private information. During the time of exposure, both unauthorized individuals and cybercriminals had unlimited, unauthorized access to Defendant's computer network.

40. UNOS reported on its website that the information breached included "Social Security numbers, dates of birth, health insurance claim numbers, the date information was added to the OPTN database, and other dates related to transplant or donor services."[12] In other words, UNOS has admitted that the files exposed by UNOS contained protected health information as well as Social Security numbers along with personally identifiable information.

41. Therefore, ***Plaintiff's and Class members' Private Information was exposed and likely in the hands of cybercriminals for over 10 months before they were notified*** of UNOS's Data Breach. Time is of the essence when trying to protect against identity theft after a data breach, so early notification is critical.

42. Upon information and belief, the Private Information stored on UNOS's network was not encrypted.

---

[11] *See* Notice Letter, Ex. A.
[12] *Id.* (Last accessed November 2, 2023).

43. In the case of UNOS specifically, the risks are far greater than simply fraud. As explained by Senators Wyden and Grassley in their March 20, 2023 letter "UNOS is the sole operator of the DonorNet system, which maintains the waitlist for all organ transplant candidates in the United States. This means that *any interruption in service*—such as a ransomware attack, technical failure, or any inefficiency resulting in unnecessary delays—*has the potential to cause lethal harm* to patients across the country. The waiting list's patient population includes individuals on Medicare and Medicaid, particularly those suffering from kidney failure and receiving high-cost dialysis treatments."[13] (Emphasis added).

44. Plaintiff's Private Information was accessed and stolen in the Data Breach. Plaintiff reasonably believes her stolen Private Information is currently available for sale on the Dark Web because that is the *modus operandi* of cybercriminals who target businesses that collect highly sensitive Private Information.

45. As a result of the Data Breach, UNOS now encourages Class Members to engage in credit monitoring, fraud consultation, and identity theft restoration services, a tacit admission of the imminent risk of identity theft faced by Plaintiff

[13] https://www.grassley.senate.gov/news/news-releases/grassley-praises-hhs-action-to-restore-integrity-in-life-saving-organ-transplant-system (*See* link to letter) (last accessed September 3, 2024).

and Class members.[14]

46. UNOS is now encouraging Plaintiff and Class Members to "remain vigilant for evidence of identity theft or fraud. . . . [R]eview their bank account, financial statements and credit reports for suspicious activity, and promptly report any suspicious activity to your financial institution. Individuals can also visit the Federal Trade Commission's website on identity theft protection (identitytheft.gov) for information on how to place a fraud alert or security freeze on their credit file." This advice is an acknowledgment that the impacted individuals are subject to a substantial and imminent threat of fraud and identity theft.

47. UNOS had obligations created by statute, HIPAA, the FTC Act, contract, industry standards, and common law to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

48. UNOS could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting its equipment and computer files containing PII, and properly structuring and monitoring its collected data.

Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII.

49. UNOS acquires, collects, and stores a massive amount of Private

[14] Notice Letter, Exhibit A.

Information of individuals who are seeking organ donor or transplant services.

50. By obtaining, collecting, and using Plaintiff's and Class Members' PII for its own financial gain and business purposes, Defendant assumed legal and equitable duties and knew that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

51. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

52. Plaintiff and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

53. It is well known that PII, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect such information, including UNOS, are well aware of the risk of being targeted by cybercriminals.

54. Individuals place a high value not only on their PII, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

55. A data breach increases the risk of becoming a victim of identity theft.

Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss."[15]

56. Individuals, like Plaintiff and Class members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing your DNA for hacker's purposes.

57. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of social security number misuse.

58. The Social Security Administration has warned that "a new number

[15] "Victims of Identity Theft, 2018," U.S. Department of Justice (April 2021, NCJ 256085) available at: https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed September 3, 2024).

probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[16]

59. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[17]

60. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches since 2020. In 2022 it was determined that from 2022 to 2024, in a poll done on security executives, they have predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[18]

61. In light of high profile data breaches at other industry leading companies, including Microsoft (250 million records, December 2019), Wattpad

---

[16] https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed September 3, 2024).
[17] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed September 3, 2024).
[18] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last accessed September 3, 2024).

(268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that its computer network would be targeted by cybercriminals.

62. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

63. Despite the prevalence of public announcements of data breach and data security compromises, and despite repeated warnings directly from U.S. Senators, and its own acknowledgments of the necessity of data security, and despite its own acknowledgment of its duties to keep PII private and secure, UNOS failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

64. Defendant failed to abide by its own Privacy Policy.[19]

At All Relevant Times Defendant Had a Duty to Plaintiff and Class Members to Properly Secure their Private Information

65. At all relevant times, UNOS had a duty to Plaintiff and Class Members

[19] https://unos.org/privacy-policy/ (last accessed September 3, 2024).

to properly secure their Private Information, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to promptly notify Plaintiff and Class Members when UNOS became aware that their PII was compromised.

66. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

67. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;
b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;
c. Monitoring for suspicious or irregular traffic to servers;
d. Monitoring for suspicious credentials used to access servers;
e. Monitoring for suspicious or irregular activity by known users;
f. Monitoring for suspicious or unknown users;
g. Monitoring for suspicious or irregular server requests;
h. Monitoring for server requests for PII;
i. Monitoring for server requests from VPNs; and
j. Monitoring for server requests from Tor exit nodes.

68. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[20] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[21]

69. The ramifications of Defendant's failure to keep consumers' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security and driver's license numbers, fraudulent use of that information and damage to victims including Plaintiff and the Class may continue for years.

The Value of Personal Identifiable Information

70. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.[22]

---

[20] 17 C.F.R. § 248.201 (2013).
[21] *Id*.
[22] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed September 3, 2024).

71. Criminals can also purchase access to entire company's data breaches from $900 to $4,500.[23]

72. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[24]

73. Attempting to change or cancel a stolen Social Security number is difficult if not nearly impossible. An individual cannot obtain a new Social Security number without evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new

---

[23] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/(last accessed September 3, 2024).
[24] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed September 3, 2024).

number.

74. Even a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[25]

75. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[26]

76. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[27]

---

[25] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed September 3, 2024).

[26] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed September 3, 2024).

[27] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1 (last accessed September 3, 2024).

77. Given the nature of this Data Breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of devastating ways. Indeed, cybercriminals who possess stolen Class Members' PII can easily obtain Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

78. The Private Information compromised in this Data Breach is static and difficult, if not impossible, to change (such as Social Security numbers).

79. Moreover, UNOS has offered no identity theft monitoring and identity theft protection although victims are likely to face many years of identity theft.

80. Furthermore, Defendant's failure to offer credit monitoring and mere advice to Plaintiff and Class Members squarely places the burden on Plaintiff and Class Members, rather than on the Defendant, to monitor and report suspicious activities to law enforcement. In other words, Defendant expects Plaintiff and Class Members to protect themselves from its tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the breach, Defendant merely sent instructions to Plaintiff and Class Members about actions they can affirmatively take to protect themselves.

81. Victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely

fail to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

82. Furthermore, even when all necessary data is not in a single data breach, criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[28]

83. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

84. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such

[28] "Fullz" is slang for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the Dark Web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/ (last visited September 5, 2024).

as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

85. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the Data Breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

86. Thus, even if certain information (such as telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

87. After collected, the comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

88. The injuries to Plaintiff and Class Members were directly and proximately caused by UNOS's failure to implement or maintain adequate data security measures for the victims of its Data Breach.

Defendant Failed to Comply with FTC Guidelines

89. Federal and State governments have established security standards and issued recommendations to mitigate the risk of data breaches and the resulting harm

to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[29]

90. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[30] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

91. The FTC emphasizes that early notification to data breach victims reduces injuries: "If you quickly notify people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused" and "thieves who have stolen names and Social Security numbers can use that information not only to sign up for new accounts in the victim's name,

---

[29] Federal Trade Commission, *Start With Security, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed September 3, 2024).

[30] Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed September 3, 2024).

but also to commit tax identity theft. People who are notified early can take steps to limit the damage."[31]

92. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[32]

93. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.
b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.
c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.
d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.
e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be

[31] https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business (last accessed September 3, 2024).
[32] *See* FTC, *Start With Security*, *supra*.

particularly vulnerable to a variety of hack attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

94. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice

prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

95. Because Class Members entrusted Defendant with their PII, Defendant had, and has, a duty to the Plaintiff and Class Members to keep their PII secure.

96. Plaintiff and the other Class Members reasonably expected that when they provide PII to Defendant, UNOS would safeguard their PII.

97. UNOS was at all times fully aware of its obligation to protect the personal, financial, and health data of consumers, including Plaintiff and members of the Class. UNOS was also aware of the significant repercussions if it failed to do so. Its own Privacy Policy, quoted above, acknowledges this awareness.

98. UNOS's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiff's and Class Members' Social Security numbers, and other highly sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Plaintiff and Class Members Have Suffered Concrete Injury as a Result of Defendant's Inadequate Security and the Data Breach it Allowed.

99. Plaintiff and Class Members reasonably expected that Defendant would provide adequate security protections for their Private Information, and Class

Members provided Defendant with sensitive personal information, including their names, addresses, and Social Security numbers, and extensive health histories.

100. Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. Plaintiff and other individuals whose PII was entrusted with UNOS understood and expected that, as part of that business relationship, they would receive data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received data security that was of a lesser value than what they reasonably expected. As such, Plaintiff and the Class Members suffered pecuniary injury.

101. Cybercriminals intentionally attack and exfiltrate PII to exploit it. Thus, Class Members are now, and for the rest of their lives will be, at a heightened and substantial risk of identity theft. Plaintiff and Class Members have also incurred (and will continue to incur) damages in the form of, inter alia, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

102. The cybercriminals who obtained the Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets" or on the "dark web." Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including:

- obtaining employment;

- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

103. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

104. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and the other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

105. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for fraudulent misuse of this information to be detected.

106. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach." Javelin Strategy & Research, a leading provider of quantitative

and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[33] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

107. As a result of the Data Breach, Plaintiff and Class Members have already suffered injuries, and each are at risk of a substantial and imminent risk of future identity theft.

108. UNOS admits that its systems allowed actual exposure of Plaintiff and Class Members' Private Information stored on the UNOS network. Its exposure to unauthorized persons is not theoretical here.[34]

Data Breaches Put Consumers at an Increased Risk Of Fraud and Identify Theft

109. Data Breaches such as the one experienced by Plaintiff and Class are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

---

[33] The Consumer Data Insecurity Report: Examining The Data Breach- Identity Fraud Paradigm In Four Major Metropolitan Areas, (*available at* https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf) (last accessed September 3, 2024).
[34] See Notice Letter, Ex. A.

110. In 2019, the United States Government Accountability Office released a report addressing the steps consumers can take after a data breach.[35] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. *See* GAO chart of consumer recommendations, reproduced and attached as Exhibit B. It is clear from the GAO's recommendations that the steps Data Breach victims (like Plaintiff and Class) must take after a breach like Defendant's are both time consuming and of only limited and short-term effectiveness.

111. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record," discussing the same in a 2007 report as well ("2007 GAO Report").[36]

112. The FTC, like the GAO (*see* Exhibit B), recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their

---

[35] https://www.gao.gov/assets/gao-19-230.pdf (last accessed September 3, 2024). *See* attached as Ex. B.

[36] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last accessed November 2, 2023) ("2007 GAO Report").

identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[37]

113. Theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[38]

114. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which has conducted studies regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See 2007 GAO Report, at p. 29.

115. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised,

---

[37] *See* https://www.identitytheft.gov/Steps (last accessed September 3, 2024).
[38] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

criminals often trade the information on the "cyber black-market" for years.

116. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

117. As the HHS warns, "PHI can be exceptionally valuable when stolen and sold on a black market, as it often is. PHI, once acquired by an unauthorized individual, can be exploited via extortion, fraud, identity theft and data laundering. At least one study has identified the value of a PHI record at $1000 each."[39]

Plaintiff White's Experience

118. Plaintiff Lisa White is, and at all times relevant to this complaint, a resident and citizen of the State of Tennessee.

119. Plaintiff White is an organ donor who registered with UNOS in approximately 2007. At that time, UNOS required that Plaintiff White provide it with an extensive amount of her Private Information, including but not limited to her Social Security number and her lifetime medical history.

---

[39] https://www.hhs.gov/sites/default/files/cost-analysis-of-healthcare-sector-data-breaches.pdf at 2 (citations omitted) (last accessed September 3, 2024).

120. Just after August 21, 2024, Plaintiff White received the Notice of Data Breach letter, delivered by the US Mail, which indicated that UNOS had known about the Data Breach for over nine months before notifying her. The letter also informed her that her private information had "been stored in the [non-private] test environment since [its] creation in 2007 and 2011." *See* Ex. A.

121. The letter stated that the exposed information included her "Social Security number, date of birth, health insurance claim number, the date your information was added to the OPTN database, and other dates related to transplant or donor services" but did not expand on whether additional information was stolen as well. *See* Ex. A.

122. Plaintiff White is alarmed by this Data Breach, especially since she is well-aware of the extensive medical history that was collected and stored during the process of being considered as an organ donor. Equally detrimental is the fact that her Social Security number was specifically identified as among the breached data on UNOS's computer system.

123. Becoming an organ donor as Plaintiff White did in 2009, is a serious, life-altering event that is altruistic but also medically grueling. Providing extensive medical history and testing to UNOS and related organizations is time consuming and extremely private. Plaintiff White provided this information to UNOS with the absolute and reasonable expectation that her Private Information would be

absolutely secure, as UNOS promised her in 2007.

124. UNOS's failure to secure Plaintiff White's Private Information is an extreme breach of her personal privacy.

125. In response to UNOS's Notice of Data Breach, Plaintiff has already spent hours of otherwise productive time dealing with the consequences of the Data Breach, and she will continue to have to self-monitor her medical and financial accounts for indications that her Private Information is in the public sphere.

126. Plaintiff is very careful about sharing her Private Information, especially as related to her medical history and organ donation as well as her Social Security number. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Due to the prevalence of data breaches, for the past 5 years or so, she has regularly refused to provide her Social Security number to medical organizations for treatment even when asked.

127. Plaintiff has suffered actual injury and damages as a result of the Data Breach. Plaintiff would not have provided UNOS with her Private Information had UNOS disclosed that it lacked data security practices adequate to safeguard PII, that it would be so reckless as to leave Private Information unencrypted and exposed for decades.

128. Plaintiff suffered actual injury in the form of damages and diminution in the value of her PII—a form of intangible property that she entrusted to UNOS.

129. Plaintiff has already suffered lost time, extreme loss of privacy, annoyance, interference, and inconvenience as a result of the Data Breach. She has anxiety and increased concerns for the loss of her privacy, especially her medical history and Social Security number.

130. Plaintiff White reasonably believes that her Private Information may have already been sold by cybercriminals. Had she been notified of UNOS's security failures in a more timely manner, she could have attempted to mitigate her injuries by requesting the deletion or encryption of her Private Information for UNOS's computer system.

131. Plaintiff White has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her exposed Private Information, especially her Social Security number, being exposed to unauthorized third-parties.

132. Plaintiff has a continuing interest in ensuring that her Private Information, which upon information and belief remains backed up and in UNOS's possession, is protected and safeguarded from future exposure and breaches.

CLASS ACTION ALLEGATIONS

133. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class").

134. Plaintiff proposes the following Class definition, subject to amendment

as appropriate:

> All individuals whose Private Information was maintained on The United Network for Organ Sharing's computer systems and who were sent a Notice of Data Privacy Incident in or about August 2024.

135. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

136. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

137. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. Based on information and belief, the Class is believed to include **at least 1.5 million individuals** whose data was compromised in Data Breach.

138. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

A. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

B. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

C. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

D. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

E. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

F. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

G. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

H. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

I. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

J. Whether Defendant's conduct was negligent;

K. Whether Defendant failed to provide notice of the Data Breach in a

timely manner; and

L. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

139. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach.

140. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating Class actions.

141. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' Private Information was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

142. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost

of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

143. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

144. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;
- Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;
- Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

- Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and
- Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

145. All members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by UNOS.

146. Finally, Defendant disregarded the rights of Plaintiff and Class members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient private information; failing to take standard and reasonably available steps to prevent the data breach; failing to properly train its staff and employees on proper security measures; and failing to provide plaintiffs and class members prompt notice of the data breach.

CAUSES OF ACTION

FIRST COUNT
Negligence
(On behalf of Plaintiff and All Class Members)

147. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

148. Defendant gathered and stored the Private Information of Plaintiff and Class Members as part of the regular course of its business operations. Plaintiff and Class Members were entirely dependent on Defendant to use reasonable measures to safeguard their Private Information and were vulnerable to the foreseeable harm described herein should Defendant fail to safeguard their Private Information.

149. By collecting and storing this data in its computer property, and sharing it, and using it for commercial gain, Defendant assumed a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

150. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements

discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

151. Defendant had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

152. Plaintiff and the Class are within the class of persons that HIPAA and the FTC Act were intended to protect.

153. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

154. Defendant gathered and stored the Private Information of Plaintiff and Class Members as part of its business managing organ donations in the United States, facilitating organ transplants, and maintaining the organ donation waitlists.

155. Defendant violated the FTC Act by failing to use reasonable measures to protect the Private Information of Plaintiff and Class Members and by not complying with applicable industry standards, as described herein.

156. Defendant breached its duties to Plaintiff and Class Members under the

FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiff's and Class Members' Private Information, and by failing to provide prompt notice without reasonable delay.

157. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and those who received its services, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach or data breach.

158. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare, medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

159. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

160. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also

because Defendant is bound by industry standards to protect confidential Private Information.

161. Defendant had full knowledge of the sensitivity of the Private Information, the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully disclosed, and the importance of adequate security.

162. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class members had no ability to protect their Private Information that was in Defendant's possession.

163. Defendant was in a special relationship with Plaintiff and Class Members with respect to the hacked information because the aim of Defendant's data security measures was to benefit Plaintiff and Class Members by ensuring that their personal information would remain protected and secure. Only Defendant was in a position to ensure that its systems were sufficiently secure to protect Plaintiff's and Class Members' Private Information. The harm to Plaintiff and Class members from its exposure was highly foreseeable to Defendant.

164. Defendant owed Plaintiff and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing their Private Information, including taking action to reasonably safeguard such data and providing notification

to Plaintiff and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

165. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. See Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

166. Defendant had duties to protect and safeguard the Private Information of Plaintiff and the Class from being vulnerable to compromise by taking common-sense precautions when dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiff and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant' networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class members' Private Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiff's and Class Members' Private Information in its possession by using reasonable and adequate security procedures and

systems; and

c. To promptly notify Plaintiff and Class Members of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their Private Information.

167. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Private Information that had been entrusted to them.

168. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class Members' Private Information. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the Private Information in its possession;

b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;

d. Failing to adequately train its employees to not store unencrypted Private Information in their personal files longer than absolutely

necessary for the specific purpose that it was sent or received;

e. Failing to consistently enforce security policies aimed at protecting Plaintiff's and Class Members' Private Information;

f. Failing to mitigate the harm caused to Plaintiff and the Class Members;

g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. Failing to promptly notify Plaintiff and Class Members of the Data Breach that affected their Private Information.

169. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

170. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

171. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiff and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiff and Class Members while it was within Defendant's possession and control.

172. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to securing their Private Information and mitigating damages.

173. As a result of the Data Breach, Plaintiff and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to the fraudulent use of the Private Information, and closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies.

174. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

175. The damages Plaintiff and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

176. Plaintiff and the Class have suffered injury and are entitled to actual damages in amounts to be proven at trial.

SECOND COUNT
Breach of Implied Contract
(On Behalf of Plaintiff and All Class Members)

177. Plaintiff re-alleges and incorporates by the paragraphs above as if fully set forth herein.

178. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of receiving organ donation services provided by Defendant.

179. Plaintiff and Class Members provided their PII to Defendant or its third-party agents in exchange for UNOS's services. In exchange for the PII, Defendant promised to protect their PII from unauthorized disclosure.

180. Defendant promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

181. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

182. When Plaintiff and Class Members provided their Private Information

to Defendant as a condition of relationship, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

183. Defendant required Class Members to provide their Private Information as part of Defendant's regular business practices.

184. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

185. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

186. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

187. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

188. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

189. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

190. Plaintiff and Class Members are also entitled to nominal damages for the breach of implied contract.

191. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate long term credit monitoring to all Class Members for a period of no less than ten years.

THIRD COUNT
Unjust Enrichment
(On Behalf of Plaintiff and All Class Members)

192. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

193. Plaintiff and Class Members conferred a monetary benefit on Defendant in the form of the provision of their Private Information and Defendant would be unable to engage in its regular course of business without that Private Information.

194. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiff and Class Members and accepted that monetary benefit.

195. However, acceptance of the benefit under the facts and circumstances

outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

196. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures.

197. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

198. If Plaintiff and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

199. Plaintiff and Class Members have no adequate remedy at law.

200. As a direct and proximate result of Defendant's conduct, Plaintiff and

Class Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

201. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

202. Defendant should be compelled to disgorge into a common fund or

constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

FOURTH COUNT
Declaratory Judgment
(On Behalf of Plaintiff and All Class Members)

203. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

204. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

205. An actual controversy has arisen in the wake of the UNOS data breach regarding its present and prospective common law and other duties to reasonably safeguard individuals' Private Information and whether UNOS is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their Private Information.

206. Plaintiff alleges that UNOS's data security measures remain inadequate. Plaintiff will continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

207. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. UNOS continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, HIPAA, and various state statutes;

b. UNOS continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

208. The Court also should issue corresponding prospective injunctive relief requiring UNOS to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information.

209. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at UNOS. The risk of another such breach is real, immediate, and substantial. If another breach at UNOS occurs, Plaintiff and class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

210. The hardship to Plaintiff and class members if an injunction does not issue exceeds the hardship to UNOS if an injunction is issued. Among other things,

if another massive data breach occurs at UNOS, Plaintiff and class members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to UNOS of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and UNOS has a pre-existing legal obligation to employ such measures.

211. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at UNOS, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures of its Data Breach to Plaintiff and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate

methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. For declaratory relief as requested;

F. Ordering Defendant to pay for lifetime credit monitoring services for Plaintiff and the Class;

G. For an award of actual damages, compensatory damages, and statutory damages, in an amount to be determined, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: September 5, 2024

Respectfully submitted,

/s/David Hilton Wise
David Hilton Wise, VA Bar No. 30828
William N. Evans, VA Bar No. 87506
WISE LAW FIRM PLC
10640 Page Avenue, Suite 320
Fairfax, Virginia 22030
Phone: 703-934-6377
dwise@wiselaw.pro
wevans@wiselaw.pro

Danielle L. Perry*
Ra O. Amen*
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
Email: dperry@masonllp.com
Email: ramen@masonllp.com

Attorneys for Plaintiff

**pro hac vice or applications for admission to be filed*